P14683-A

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　４月　３日

出願番号
Application Number: 特願２００１－１０４３３１

出願人
Applicant(s): 日本電信電話株式会社

２００１年　６月１３日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０５５４３８

【書類名】　特許願

【整理番号】　NTTH127195

【提出日】　平成13年 4月 3日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 15/21

G06F 15/62

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　重松　智志

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　斎藤　賢一

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　羽田野　孝裕

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　久良木　億

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　島村　俊重

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　町田　克之

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【代理人】

【識別番号】　100064621

【弁理士】

【氏名又は名称】　山川　政樹

【電話番号】　03-3580-0961

【手数料の表示】

【予納台帳番号】　006194

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9701512

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　携帯型端末システム、生体認証装置及び携帯型端末装置

【特許請求の範囲】

【請求項１】　携帯型端末装置と生体認証装置とからなる携帯型端末システムであって、

前記生体認証装置は、自装置を所持するユーザの生体情報を読み取る生体情報読取手段と、

予め登録された正規ユーザの生体情報とこの正規ユーザの個人情報とを記憶する第１の記憶手段と、

前記生体情報読取手段で読み取られた生体情報と前記第１の記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、前記第１の記憶手段に記憶された個人情報を前記携帯型端末装置に送信する第１の処理装置とを有し、

前記携帯型端末装置は、前記生体認証装置から送信された個人情報を記憶する第２の記憶手段と、

この第２の記憶手段に記憶された個人情報を用いて通信処理又はデータ処理を行う第２の処理手段とを有することを特徴とする携帯型端末システム。

【請求項２】　携帯型端末装置と生体認証装置とからなる携帯型端末システムであって、

前記生体認証装置は、自装置を所持するユーザの生体情報を読み取る生体情報読取手段と、

予め登録された正規ユーザの生体情報とこの正規ユーザがサービス提供を受けるのに必要なサービス情報とを記憶する第１の記憶手段と、

前記生体情報読取手段で読み取られた生体情報と前記第１の記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、前記第１の記憶手段に記憶されたサービス情報を前記携帯型端末装置に送信する第１の処理装置とを有し、

前記携帯型端末装置は、前記生体認証装置から送信されたサービス情報を記憶する第２の記憶手段と、

この第２の記憶手段に記憶されたサービス情報を用いて通信処理又はデータ処理を行う第２の処理手段とを有することを特徴とする携帯型端末システム。

【請求項３】　請求項１記載の携帯型端末システムにおいて、

前記個人情報は、前記正規ユーザの個人識別番号を含み、

前記携帯型端末装置の第２の処理手段は、前記第２の記憶手段に前記個人情報が格納された後、この個人情報に含まれる前記個人識別番号を用いてネットワークとの回線接続を行うことを特徴とする携帯型端末システム。

【請求項４】　請求項２記載の携帯型端末システムにおいて、

前記サービス情報は、ウエブサイトにログインする際に使用されるパスワードを含み、

前記携帯型端末装置の第２の処理手段は、前記第２の記憶手段に前記サービス情報が格納された後、ネットワークを介してアクセスしたウエブサイトに対応するパスワードを前記サービス情報中から取得し、取得したパスワードをアクセス先のウエブサイトに送信することを特徴とする携帯型端末システム。

【請求項５】　自装置を所持するユーザの生体情報を読み取る生体情報読取手段と、

予め登録された正規ユーザの生体情報とこの正規ユーザの個人情報とを記憶する記憶手段と、

前記生体情報読取手段で読み取られた生体情報と前記記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、前記記憶手段に記憶された個人情報を携帯型端末装置に送信する処理装置とを有し、

前記個人情報を保持していない前記携帯型端末装置に前記認証結果が照合一致を示す場合のみ前記個人情報を送信することにより、前記個人情報を用いた通信処理又はデータ処理を許可することを特徴とする生体認証装置。

【請求項６】　自装置を所持するユーザの生体情報を読み取る生体情報読取手段と、

予め登録された正規ユーザの生体情報とこの正規ユーザがサービス提供を受けるのに必要なサービス情報とを記憶する記憶手段と、

前記生体情報読取手段で読み取られた生体情報と前記記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、前記記憶手段に記憶されたサービス情報を携帯型端末装置に送信する処理装置とを有し、

前記サービス情報を保持していない前記携帯型端末装置に前記認証結果が照合一致を示す場合のみ前記サービス情報を送信することにより、前記サービス情報を用いた通信処理又はデータ処理を許可することを特徴とする生体認証装置。

【請求項７】　請求項５記載の生体認証装置において、

前記個人情報は、前記携帯型端末装置とネットワークとの回線接続に必要な前記正規ユーザの個人識別番号を含むことを特徴とする生体認証装置。

【請求項８】　請求項６記載の生体認証装置において、

前記サービス情報は、前記携帯型端末装置からネットワークを介してウエブサイトにログインする際に使用されるパスワードを含むことを特徴とする生体認証装置。

【請求項９】　ユーザの生体情報を用いて本人認証を行い、認証結果が照合一致を示す場合のみ正規ユーザの個人情報を送信する生体認証装置から、前記個人情報を受信して記憶する記憶手段と、

この記憶手段に記憶された個人情報を用いて通信処理又はデータ処理を行う処理手段とを有し、

前記生体認証装置に記憶された前記個人情報を受信した場合のみ、前記個人情報を用いた通信処理又はデータ処理を行うことを特徴とする携帯型端末装置。

【請求項１０】　ユーザの生体情報を用いて本人認証を行い、認証結果が照合一致を示す場合のみ正規ユーザがサービス提供を受けるのに必要なサービス情報を送信する生体認証装置から、前記サービス情報を受信して記憶する記憶手段と、

この記憶手段に記憶されたサービス情報を用いて通信処理又はデータ処理を行う処理手段とを有し、

前記生体認証装置に記憶された前記サービス情報を受信した場合のみ、前記サービス情報を用いた通信処理又はデータ処理を行うことを特徴とする携帯型端末

装置。

【請求項１１】　請求項９記載の携帯型端末装置において、

前記個人情報は、前記正規ユーザの個人識別番号を含み、

前記携帯型端末装置の処理手段は、前記記憶手段に前記個人情報が格納された後、この個人情報に含まれる前記個人識別番号を用いてネットワークとの回線接続を行うことを特徴とする携帯型端末装置。

【請求項１２】　請求項１０記載の携帯型端末装置において、

前記サービス情報は、ウエブサイトにログインする際に使用されるパスワードを含み、

前記携帯型端末装置の処理手段は、前記記憶手段に前記サービス情報が格納された後、ネットワークを介してアクセスしたウエブサイトに対応するパスワードを前記サービス情報中から取得し、取得したパスワードをアクセス先のウエブサイトに送信することを特徴とする携帯型端末装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ユーザの生体情報を用いて本人認証を行う例えば携帯電話機等の携帯型端末システム、生体認証装置及び携帯型端末装置に関するものである。

【０００２】

【従来の技術】

従来より、携帯電話機等の携帯型端末装置には、電話番号、電子メールアドレス等の個人情報が保存されている。このような個人情報が正規のユーザ以外の第三者に漏洩するのを防ぐため、個人情報へのデータアクセス処理にパスワードを設定して、第三者が個人情報に不正にアクセスすることを防止していた。

また、近年、携帯型端末装置からネットワークを介してウエブサイトにアクセスし、例えば商品購入などの電子商取引を行うことが可能となった。このような電子商取引においても、ユーザの正当性確認のためにパスワードが用いられている。

【０００３】

【発明が解決しようとする課題】

しかしながら、従来の携帯型端末装置では、正規ユーザ以外の第三者がデータアクセスに必要なパスワードを不正に取得すると、携帯型端末装置に記憶された個人情報にアクセスすることが可能となるため、個人情報が漏洩する可能性があった。

同様に、正規ユーザ以外の第三者がサービス情報、例えば電子商取引に必要なパスワードを不正に取得すると、第三者は正規ユーザになりすまして電子商取引を行うことが可能となるため、携帯型端末装置が不正に使用されて正規ユーザに課金がなされるといった問題が起こる可能性があった。

本発明は、上記課題を解決するためになされたもので、個人情報及びサービス情報の漏洩と不正な電子商取引とを防止することができる携帯型端末システム、生体認証装置及び携帯型端末装置を提供することを目的とする。

【０００４】

【課題を解決するための手段】

本発明の携帯型端末システムは、携帯型端末装置（１）と生体認証装置（２）とからなり、前記生体認証装置は、自装置を所持するユーザの生体情報を読み取る生体情報読取手段（２２）と、予め登録された正規ユーザの生体情報とこの正規ユーザの個人情報とを記憶する第１の記憶手段（２３）と、前記生体情報読取手段で読み取られた生体情報と前記第１の記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、前記第１の記憶手段に記憶された個人情報を前記携帯型端末装置に送信する第１の処理装置（２４）とを有し、前記携帯型端末装置は、前記生体認証装置から送信された個人情報を記憶する第２の記憶手段（１５）と、この第２の記憶手段に記憶された個人情報を用いて通信処理又はデータ処理を行う第２の処理手段（１４）とを有するものである。

また、本発明の携帯型端末システムは、携帯型端末装置と生体認証装置とからなり、前記生体認証装置は、自装置を所持するユーザの生体情報を読み取る生体情報読取手段と、予め登録された正規ユーザの生体情報とこの正規ユーザがサービス提供を受けるのに必要なサービス情報とを記憶する第１の記憶手段と、前記

生体情報読取手段で読み取られた生体情報と前記第１の記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、前記第１の記憶手段に記憶されたサービス情報を前記携帯型端末装置に送信する第１の処理装置とを有し、前記携帯型端末装置は、前記生体認証装置から送信されたサービス情報を記憶する第２の記憶手段と、この第２の記憶手段に記憶されたサービス情報を用いて通信処理又はデータ処理を行う第２の処理手段とを有するものである。

また、本発明の携帯型端末システムの１構成例において、前記個人情報は、前記正規ユーザの個人識別番号を含み、前記携帯型端末装置の第２の処理手段は、前記第２の記憶手段に前記個人情報が格納された後、この個人情報に含まれる前記個人識別番号を用いてネットワークとの回線接続を行うものである。

また、本発明の携帯型端末システムの１構成例において、前記サービス情報は、ウエブサイトにログインする際に使用されるパスワードを含み、前記携帯型端末装置の第２の処理手段は、前記第２の記憶手段に前記サービス情報が格納された後、ネットワークを介してアクセスしたウエブサイトに対応するパスワードを前記サービス情報中から取得し、取得したパスワードをアクセス先のウエブサイトに送信するものである。

【０００５】

また、本発明の生体認証装置は、自装置を所持するユーザの生体情報を読み取る生体情報読取手段と、予め登録された正規ユーザの生体情報とこの正規ユーザの個人情報とを記憶する記憶手段と、前記生体情報読取手段で読み取られた生体情報と前記記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、前記記憶手段に記憶された個人情報を携帯型端末装置に送信する処理装置とを有し、前記個人情報を保持していない前記携帯型端末装置に前記認証結果が照合一致を示す場合のみ前記個人情報を送信することにより、前記個人情報を用いた通信処理又はデータ処理を許可するものである。

また、本発明の生体認証装置は、自装置を所持するユーザの生体情報を読み取る生体情報読取手段と、予め登録された正規ユーザの生体情報とこの正規ユーザ

がサービス提供を受けるのに必要なサービス情報とを記憶する記憶手段と、前記生体情報読取手段で読み取られた生体情報と前記記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、前記記憶手段に記憶されたサービス情報を携帯型端末装置に送信する処理装置とを有し、前記サービス情報を保持していない前記携帯型端末装置に前記認証結果が照合一致を示す場合のみ前記サービス情報を送信することにより、前記サービス情報を用いた通信処理又はデータ処理を許可するものである。

また、本発明の生体認証装置の１構成例において、前記個人情報は、前記携帯型端末装置とネットワークとの回線接続に必要な前記正規ユーザの個人識別番号を含むものである。

また、本発明の生体認証装置の１構成例において、前記サービス情報は、前記携帯型端末装置からネットワークを介してウエブサイトにログインする際に使用されるパスワードを含むものである。

【０００６】

また、本発明の携帯型端末装置は、ユーザの生体情報を用いて本人認証を行い、認証結果が照合一致を示す場合のみ正規ユーザの個人情報を送信する生体認証装置から、前記個人情報を受信して記憶する記憶手段と、この記憶手段に記憶された個人情報を用いて通信処理又はデータ処理を行う処理手段とを有し、前記生体認証装置に記憶された前記個人情報を受信した場合のみ、前記個人情報を用いた通信処理又はデータ処理を行うものである。

また、本発明の携帯型端末装置は、ユーザの生体情報を用いて本人認証を行い、認証結果が照合一致を示す場合のみ正規ユーザがサービス提供を受けるのに必要なサービス情報を送信する生体認証装置から、前記サービス情報を受信して記憶する記憶手段と、この記憶手段に記憶されたサービス情報を用いて通信処理又はデータ処理を行う処理手段とを有し、前記生体認証装置に記憶された前記サービス情報を受信した場合のみ、前記サービス情報を用いた通信処理又はデータ処理を行うものである。

また、本発明の携帯型端末装置の１構成例において、前記個人情報は、前記正規ユーザの個人識別番号を含み、前記携帯型端末装置の処理手段は、前記記憶手

段に前記個人情報が格納された後、この個人情報に含まれる前記個人識別番号を用いてネットワークとの回線接続を行うものである。

また、本発明の携帯型端末装置の１構成例において、前記サービス情報は、ウエブサイトにログインする際に使用されるパスワードを含み、前記携帯型端末装置の処理手段は、前記記憶手段に前記サービス情報が格納された後、ネットワークを介してアクセスしたウエブサイトに対応するパスワードを前記サービス情報中から取得し、取得したパスワードをアクセス先のウエブサイトに送信するものである。

【０００７】

【発明の実施の形態】

［実施の形態の１］

以下、本発明の実施の形態について図面を参照して詳細に説明する。図１は本発明の第１の実施の形態となる携帯型端末システムの外観図である。図１（ａ）に示すように、携帯型端末システムは、システムの本体である携帯型端末装置１と、生体認証装置２とから構成される。携帯型端末装置１には、生体認証装置２を差し込むためのスロットが設けられており、このスロットに生体認証装置２を差し込んで携帯型端末装置１と生体認証装置２とを接続し、生体認証装置２により本人認証が行われると携帯型端末装置１にアクセスできるようになっている（図１（ｂ））。

【０００８】

図２は携帯型端末装置１の構成を示すブロック図である。携帯型端末装置１は、生体認証装置２との接続のために前記スロットに配設された外部端子１０と、生体認証装置２とのインタフェースとなるインタフェース装置１１と、例えば基地局等との間で電波の送受信を行うアンテナ１２と、アンテナ１２を介して音声、画像又はテキスト等のデータの送受信を行う通信手段である無線送受信装置１３と、端末装置全体を制御し、送受信データを処理する処理装置１４と、情報記憶のための記憶装置１５と、複数のキースイッチからなる入力装置１６と、画面表示を行う液晶パネル等からなる表示装置１７と、ユーザの音声をマイクロホンで集音して音声データに変換する音声入力装置１８と、受信された音声データを

アナログ音声信号に変換してスピーカから出力する音声出力装置１９とを有している。

【０００９】

図３（ａ）は生体認証装置２の斜視図、図３（ｂ）は生体認証装置２の構成を示すブロック図である。生体認証装置２は、携帯型端末装置１との接続のための外部端子２０と、携帯型端末装置１とのインタフェースとなるインタフェース装置２１と、ユーザの生体情報を読み取る生体情報読取手段となるセンサ２２と、予め登録された正規ユーザの生体情報とこの正規ユーザの個人情報及びサービス情報とを記憶する記憶装置２３と、センサ２２で読み取った生体情報と記憶装置２３に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、記憶装置２３に記憶された個人情報及びサービス情報を携帯型端末装置１に送信する処理装置２４とを有している。生体認証装置２は、外部端子２０以外の全ての機能が１つのＬＳＩチップに搭載されている形でもよいし、その他の構成でもよい。

【００１０】

以下、本実施の形態の携帯型端末システムの動作を図４を用いて説明する。ここでは、ユーザの生体情報として指紋を用いるものとして説明する。まず、携帯型端末装置１を使って電話をかけようとするユーザは、自身が所持する生体認証装置２を携帯型端末装置１のスロットに差し込む（図４ステップ１０１）。これにより、携帯型端末装置１と生体認証装置２とが外部端子１０，２０を介して接続される。

【００１１】

生体認証装置２の記憶装置２３には、正規ユーザの指紋画像データと、この正規ユーザの個人識別番号、氏名、住所、生年月日及びクレジットカード番号等の個人情報と、電話帳のデータ、電子メールアドレス帳のデータ及びパスワード等のサービス情報とが予め記憶されている。個人識別番号は、通信事業者が正規ユーザに付与した識別番号であり、例えば正規ユーザの電話番号である。携帯型端末装置１の記憶装置１５には、通信処理やデータ処理等の携帯型端末装置１の動作に必要なプログラムが格納されているが、前記個人情報及びサービス情報は格

納されていない。

【００１２】

次に、ユーザは、生体認証装置２による本人認証を受けるべく、センサ２２上に指を載せる（ステップ１０２）。センサ２２は、ユーザの指紋画像を読み取る（ステップ１０３）。処理装置２４は、センサ２２によって読み取られた指紋画像と記憶装置２３に予め登録された正規ユーザの指紋画像とを照合して本人認証を行う（ステップ１０４）。処理装置２４における認証アルゴリズムには様々な方式があり、センサ２２で読み取った指紋画像の特徴点を抽出して正規ユーザの指紋画像の特徴点と比較する特徴点抽出方式や、センサ２２で読み取った指紋画像を正規ユーザの指紋画像と直接比較するパタンマッチング方式などがある。

【００１３】

処理装置２４は、指紋画像が一致し、認証結果がＯＫである場合（ステップ１０５においてＹＥＳ）、生体認証装置２を所持するユーザを正規ユーザと判断して、このユーザによる携帯型端末装置１へのアクセスを許可する。すなわち、処理装置２４は、個人識別番号等の個人情報と、電話帳のデータ、電子メールアドレス帳のデータ及びパスワード等のサービス情報とを記憶装置２３から読み出し、読み出した個人情報及びサービス情報をインタフェース装置２１を介して携帯型端末装置１に送出する（ステップ１０６）。また、処理装置２４は、指紋画像が一致せず、認証結果がＮＧである場合、生体認証装置２を所持するユーザが正規ユーザではない判断して、携帯型端末装置１への個人情報及びサービス情報の送出を拒否する（ステップ１０７）。

【００１４】

次に、携帯型端末装置１の処理装置１４は、生体認証装置２から送られた個人情報及びサービス情報をインタフェース装置１１を介して受信し記憶装置１５に格納する（ステップ１０８）。記憶装置１５に個人情報及びサービス情報が格納されることにより、携帯型端末装置１を使用することが可能になる（ステップ１０９）。

【００１５】

ステップ１０９において、例えばユーザが入力装置１６を操作して電話帳のデ

ータから着信先の電話番号を選択し、入力装置１６の発信ボタンを押下すると、処理装置１４は、記憶装置１５に記憶された個人識別番号と選択された着信先電話番号とを無線送受信装置１３に出力する。無線送受信装置１３は、個人識別番号と着信先電話番号とを無線信号に変換してアンテナ１２に出力し、アンテナ１２は、無線信号をネットワーク（移動網の基地局）に送出する。

【００１６】

携帯型端末装置１からの発呼に応じて、基地局は、受信した無線信号に含まれる着信先電話番号を基に着信先の電話機を呼び出し、着信先の電話機が応答すると、携帯型端末装置１と着信先の電話番号とを回線接続する。着信先の電話機からの音声は、アンテナ１２で受信された無線信号が無線送受信装置１３で復調され、復調された音声データが音声出力装置１９でアナログ音声信号に変換されて音声出力装置１９のスピーカから出力されることにより、再生される。

【００１７】

一方、携帯型端末装置１のユーザの音声は、音声入力装置１８のマイクロホンで集音されて音声入力装置１８で音声データに変換され、無線送受信装置１３で無線信号に変換されてアンテナ１２から送信される。以上で、携帯型端末装置１を携帯電話機として使用することが可能になる。

【００１８】

また、ステップ１０９において、ユーザが入力装置１６を操作して電子メールを作成し、電子メールアドレス帳から着信先の電子メールアドレスを選択して、入力装置１６の発信ボタンを押下すると、携帯型端末装置１の処理装置１４は、記憶装置１５に記憶された個人識別番号と所定の着信先電話番号（例えばメールサービスに割り当てられた番号）とを上記音声通信の場合と同様にネットワークに送出する。

【００１９】

ネットワークを介してメールサーバと回線接続された後、処理装置１４は、記憶装置１５に記憶されたユーザの電子メールアドレスと、選択された着信先の電子メールアドレスと、作成された電子メールの内容とを含むデータをネットワークに送出する。一方、電子メールの受信の場合には、アンテナ１２で受信された

無線信号が無線送受信装置１３で復調され、復調されたデータが処理装置１４で文字データに変換されることにより、受信した電子メールの内容が記憶装置１５に格納され、表示装置１７の画面に表示される。以上で、携帯型端末装置１を携帯型メール端末装置として使用することが可能になる。

【００２０】

また、携帯型端末装置１を画像通信の可能な端末装置として使用する場合、処理装置１４は、記憶装置１５に格納された画像データをネットワークに送出する。一方、画像データの受信の場合には、アンテナ１２で受信された無線信号が無線送受信装置１３で復調されることにより、復調された画像データが記憶装置１５に格納され、表示装置１７の画面に表示される。

【００２１】

また、電源オンやデータアクセス等の処理に予めパスワードが設定されている場合、処理装置１４は、パスワードが設定されている処理の実行をユーザから要求されたとき、パスワードの入力を要求するメッセージを表示装置１７に表示させる。そして、処理装置１４は、ユーザが入力装置１６を操作して入力したパスワードと記憶装置１５のサービス情報に含まれるパスワードとを照合して、パスワードが一致する場合のみ、要求された処理を実行する。これにより、ユーザは、携帯型端末装置１の電源オンや、個人情報又はサービス情報の閲覧・編集等の処理を行うことができる。編集した個人情報又はサービス情報を生体認証装置２に送って、生体認証装置２に記憶された個人情報又はサービス情報を更新することも可能である。

【００２２】

携帯型端末装置１の使用後、ユーザは、入力装置１６の電源ボタンを押下して携帯型端末装置１の電源をオフにする（ステップ１１０）。この電源オフに応じて、表示装置１７等への電力供給が停止される。電源ボタンがオフにされても処理装置１４への電力供給は継続されており、処理装置１４は、電源オフに応じて、記憶装置１５に記憶されている個人情報及びサービス情報を消去する（ステップ１１１）。個人情報及びサービス情報を消去するのは、携帯型端末装置１に個人情報及びサービス情報が残らないようにするためである。そして、ユーザは、

携帯型端末装置１のスロットから生体認証装置２を引き抜く（ステップ１１２）。

【００２３】

以上のように、本実施の形態では、個人情報及びサービス情報が生体認証装置２に格納されており、指紋による本人認証の結果がＯＫの場合のみ、携帯型端末装置１に個人情報及びサービス情報が送出される。このため、正規ユーザ以外の第三者がパスワードを不正に取得したとしても、指紋による本人認証の段階で携帯型端末装置１への個人情報及びサービス情報の送出が拒否されるので、第三者は、携帯型端末装置１から個人情報及びサービス情報を不正に取得することはできない。したがって、パスワードの不正取得による個人情報及びサービス情報への不正アクセスを防止することができ、セキュリティを向上させることができる。

【００２４】

また、本実施の形態では、個人識別番号（電話番号）が生体認証装置２に格納されており、指紋による本人認証の結果がＯＫの場合のみ、携帯型端末装置１に個人識別番号が送出されて付与される。このため、ユーザは、複数の携帯型端末装置１を１つの個人識別番号で使用することができ、ユーザにとっての利便性を向上させることができる。

【００２５】

また、正規ユーザ以外の第三者が正規ユーザの携帯型端末装置１と生体認証装置２とを不正に取得したとしても、指紋による本人認証の段階で携帯型端末装置１への個人識別番号送出が拒否されるので、第三者は、携帯型端末装置１を使用することができない。したがって、セキュリティを向上させることができ、携帯型端末装置１が不正に使用されて正規ユーザに課金がなされるといった問題を防ぐことができる。

【００２６】

また、本実施の形態では、１つの生体認証装置２を複数の携帯型端末装置１に差し替えて使うことができる。このため、ユーザは、個人情報及びサービス情報の管理・編集を生体認証装置２に対してのみ行えばよいので、ユーザにとっての

利便性とセキュリティとを向上させることができる。

【００２７】

なお、本実施の形態では、携帯型端末装置１の使用開始時に本人認証を行い、本人認証がＯＫの場合に、全ての個人情報及びサービス情報を生体認証装置２から携帯型端末装置１に送出するようにしているが、携帯型端末装置１の使用中にある個人情報又はサービス情報（例えば電話帳のデータ）が必要になったときに生体認証装置２による本人認証を行って、認証結果がＯＫの場合、必要とされる個人情報又はサービス情報を生体認証装置２から携帯型端末装置１に送出するようにしてもよい。

【００２８】

また、携帯型端末装置１の使用開始時に本人認証を行い、本人認証がＯＫの場合に、個人識別番号だけを生体認証装置２から携帯型端末装置１に送出するようにしてもよい。個人識別番号以外の個人情報又はサービス情報については、始めから携帯型端末装置１に記憶させておいてもよいし、前述のように必要に応じて生体認証装置２から携帯型端末装置１に送ってもよい。

【００２９】

［実施の形態の２］

図５は本発明の第２の実施の形態となる携帯型端末システムの動作を示すフローチャート図である。本実施の形態においても携帯型端末システムの構成は実施の形態の１と同様であるので、図１～図３の符号を用いて説明する。

【００３０】

生体認証装置２の記憶装置２３には、正規ユーザの指紋画像データが記憶されると共に、電子商取引のウエブサイト（以下、電子商店と呼ぶ）との間で予め取り決められたユーザの正当性確認のためのパスワードがサービス情報として記憶されている。その他の個人情報（例えば、正規ユーザの個人識別番号）やサービス情報（例えば、電話帳のデータ、電子メールアドレス帳のデータ、電源オンや個人情報にアクセスする際に必要となるパスワード等）については、携帯型端末装置１の記憶装置１５に記憶されている。

【００３１】

ユーザは、携帯型端末装置１を操作して、実施の形態の１と同様の通信処理によりインターネットに接続し、ウエブページのブラウジングを行って所望の電子商店（ウエブサーバ）にアクセスする（ステップ２０１）。これにより、表示装置１７の画面に電子商店のウエブページが表示される。続いて、ユーザは、表示されたウエブページを見て、ウエブページに掲載された商品の購入を決定すると、入力装置１６を操作してウエブページ上で商品の購入を告知する（ステップ２０２）。

【００３２】

電子商店の機能を提供する、アクセス先のウエブサーバは、携帯型端末装置１から商品の購入申し込みがあると、正規ユーザとの間で予め取り決めたパスワードの入力をユーザに要求する（ステップ２０３）。ユーザは、ウエブページに表示されたパスワードの入力要求を見て、自身が所持する生体認証装置２を携帯型端末装置１のスロットに差し込み（ステップ２０４）、生体認証装置２のセンサ２２上に指を載せる（ステップ２０５）。

【００３３】

センサ２２は、ユーザの指紋画像を読み取り（ステップ２０６）、処理装置２４は、センサ２２によって読み取られた指紋画像と記憶装置２３に予め登録された正規ユーザの指紋画像とを照合して本人認証を行い、認証結果を携帯型端末装置１に送出する（ステップ２０７）。

【００３４】

携帯型端末装置１の処理装置１４は、生体認証装置２から送られた認証結果がＯＫである場合（ステップ２０８においてＹＥＳ）、アクセス中の電子商店の識別情報（電子商店の名称又は番号）を生体認証装置２に送出する（ステップ２０９）。処理装置１４は、生体認証装置２から送られた認証結果がＮＧである場合、生体認証装置２への電子商店識別情報の送出を拒否する（ステップ２１０）。

【００３５】

生体認証装置２の処理装置２４は、認証結果がＯＫで、かつ携帯型端末装置１から電子商店識別情報を受信した場合、この電子商店識別情報に対応するパスワードを記憶装置２３から読み出し、読み出したパスワードを携帯型端末装置１に

送出する（ステップ２１１）。携帯型端末装置１の処理装置１４は、生体認証装置２から送られたパスワードをインターネットに送出する（ステップ２１２）。

【００３６】

アクセス先のウエブサーバは、携帯型端末装置１から送られたパスワードと予め登録された正規ユーザのパスワードとを照合してユーザの正当性を確認し、パスワードが一致すれば、商品の購入を申し込んだユーザを正規ユーザと判断して、このユーザの購入申し込みを受理し、購入申し込みを受理したことをアクセス元の携帯型端末装置１に通知する（ステップ２１３）。ユーザは、商品の購入申し込みが受理されたことを確認した上で、携帯型端末装置１のスロットから生体認証装置２を引き抜く（ステップ２１４）。

【００３７】

なお、生体認証装置２から送られたパスワードが携帯型端末装置１の記憶装置１５に残る可能性があるので、パスワードの使用後、実施の形態の１と同様にパスワードを消去することが望ましい。

【００３８】

以上のように本実施の形態では、電子商店にログインする際に使用されるパスワードが生体認証装置２に格納されており、指紋による本人認証の結果がＯＫの場合のみ、携帯型端末装置１にパスワードが送出されて、携帯型端末装置１から電子商店にパスワードが送出される。正規ユーザ以外の第三者が携帯型端末装置１を操作したとしても、指紋による本人認証の段階で携帯型端末装置１へのパスワード送出が拒否されるので、第三者は、正規ユーザになりすまして電子商取引を行うことはできない。したがって、セキュリティを向上させることができる。

【００３９】

なお、本実施の形態では、認証結果がＯＫの場合のみ、携帯型端末装置１から生体認証装置２に電子商店識別情報を送信するようにしているが、認証結果に関係なく電子商店識別情報を生体認証装置２に送信して、認証結果がＯＫの場合のみ、電子商店識別情報に対応するパスワードを生体認証装置２から携帯型端末装置１に送信するようにしてもよい。また、本実施の形態では、本人認証後に生体認証装置２から送出されるサービス情報をパスワードのみとしたが、パスワード

と共にクレジットカード番号やその他の個人情報が生体認証装置２から送出されるようにしてもよい。

【００４０】

［実施の形態の３］

図６は生体認証装置２内のセンサ２２の検出素子の概略的な断面を示す図である。センサ２２の検出素子は、例えばシリコンからなる半導体基板７１１上の下層絶縁膜７１２上に形成された層間絶縁膜７１４上に、たとえば８０μｍ角の複数のセンサ電極７１５と、格子状のアース電極７１６とを備え、複数のセンサ電極７１５とアース電極７１６とを、層間絶縁膜７１４表面で規定される同一平面上に配置している。

【００４１】

センサ電極７１５は、層間絶縁膜７１４上に形成されたパシベーション膜７１７で覆い、１５０μｍ間隔に複数個を備えるようにするとともに、Ａｕから構成し、膜厚１μｍ程度に形成している。パシベーション膜７１７の膜厚は３μｍ程度としたので、センサ電極７１５上には、パシベーション膜７１７が約２（＝３－１）μｍ存在している。このパシベーション膜７１７は、例えばポリイミドなどの比誘電率が４．０程度の絶縁物から構成される。上記下層絶縁膜７１２上には、センサ電極７１５にスルーホールを介して接続する配線７１３を形成する。この配線７１３により後段の回路と接続される。

【００４２】

次に、センサ２２について更に詳しく説明する。図７はセンサ２２の回路図である。図７において、Ｃｆは図６におけるセンサ電極７１５と指８１１の皮膚との間に形成される静電容量である。容量Ｃｆを形成するセンサ電極７１５はＮｃｈＭＯＳトランジスタＱ３ａのドレイン端子に接続されており、このトランジスタＱ３ａのソース端子は電流Ｉの電流源８２１の入力側に接続されている。また、センサ電極７１５とトランジスタＱ３ａとの節点Ｎ１ａには、ＮchＭＯＳトランジスタ（第１の素子）Ｑ２ａのソース端子が接続されている。このトランジスタＱ２ａのドレイン端子には、ソース端子に電源電圧ＶDDが印加されたＰchＭＯＳトランジスタ（第１のスイッチ手段）Ｑ１ａのドレイン端子と、ドレイン端子に

電源電圧ＶDDが印加されソース端子が抵抗Ｒａを介して接地に接続されたＮchＭＯＳトランジスタＱ４ａのゲート端子とが接続されている。このトランジスタＱ４ａのソース端子にインバータゲート８４１が接続されている。

【００４３】

各トランジスタＱ１ａ，Ｑ３ａのゲート端子にはそれぞれ信号ＰＲＥ（バー），ＲＥが印加される。また、トランジスタＱ２ａのゲート端子には定電圧源からバイアス電圧ＶＧが印加される。ここで、トランジスタＱ２ａが非導通状態になるゲートーソース間のしきい値電圧をＶthとすると、ＶDD＞ＶＧ－Ｖthとなるように電圧ＶDD，ＶＧが設定される。また、節点Ｎ１ａ，Ｎ２ａはそれぞれ寄生容量Ｃｐ１ａ，Ｃｐ２ａを有している。

【００４４】

容量Ｃｆにより検出素子８１０が構成され、電流源８２１とトランジスタＱ３ａとにより信号発生回路８２０が構成され、トランジスタＱ１ａ，Ｑ２ａにより信号増幅回路８３０が構成され、トランジスタＱ４ａと抵抗Ｒａとインバータゲート８４１とにより出力回路８４０が構成される。出力回路８４０は、処理装置２４と接続される。

【００４５】

図８は、図７に示したセンサ２２の動作を説明するためのタイミングチャートであり、図８（ａ）はトランジスタＱ１ａを制御する信号ＰＲＥ（バー）の電位変化を示し、図８（ｂ）はトランジスタＱ３ａを制御する信号ＲＥの電位変化を示し、図８（ｃ）は節点Ｎ１ａ，Ｎ２ａそれぞれの電位変化を示している。最初、トランジスタＱ１ａのゲート端子にはＨｉｇｈレベル（ＶDD）の信号ＰＲＥ（バー）が与えられ、トランジスタＱ３ａのゲート端子にはＬｏｗレベル（ＧＮＤ）の信号ＲＥが与えられている。したがって、このときトランジスタＱ１ａ，Ｑ３ａはともに導通していない。

【００４６】

この状態で信号ＰＲＥ（バー）がＨｉｇｈレベルからＬｏｗレベルに変化すると、トランジスタＱ１ａが導通状態になる。このときトランジスタＱ３ａは非導通状態のままであり、信号発生回路８２０は停止状態にあるから、節点Ｎ２ａの

電位がＶDDにプリチャージされる。また、トランジスタＱ２ａのゲートーソース間電圧がしきい値電圧Ｖthに達してトランジスタＱ２ａが非導通状態になるまで、節点Ｎ１ａが充電される。これにより、節点Ｎ１ａの電位がＶＧ－Ｖthにプリチャージされる。

【００４７】

プリチャージが終了した後、信号ＰＲＥ（バー）がＨｉｇｈレベルに変化すると、トランジスタＱ１ａが非導通状態になる。これと同時に信号ＲＥがＨｉｇｈレベルに変化すると、トランジスタＱ３ａが導通状態になり、信号発生回路８２０が動作状態に変化する。そして、電流源８２１により節点Ｎ１ａに充電された電荷が引き抜かれ、節点Ｎ１ａの電位がわずかに低下すると、トランジスタＱ２ａのゲートーソース間電圧がしきい値電圧Ｖthより大きくなり、トランジスタＱ２ａが導通状態に変化する。これにより節点Ｎ２ａの電荷も引き抜かれ、節点Ｎ２ａの電位低下が開始する。

【００４８】

信号ＲＥをＨｉｇｈレベルにする期間をΔｔとすると、Δｔ経過後の節点Ｎ１ａの電位低下ΔＶはＶDD－（ＶＧ－Ｖth）＋ＩΔｔ／（Ｃｆ＋Ｃｐ１ａ）になる。ここで、寄生容量Ｃｐ２ａは寄生容量Ｃｐ１ａに対して十分小さいとしている。

【００４９】

電流源８２１の電流Ｉと期間Δｔと寄生容量Ｃｐ１ａ，Ｃｐ２ａは、各々一定であるから、電位低下ΔＶは、センサ電極７１５と検出対象である指の表面８１１との間に発生する容量の値Ｃｆによって決定される。この容量値Ｃｆは、センサ電極７１５と指の表面８１１との距離によって決まるので、指紋の凹凸によって異なる。このことから、低下電位ΔＶの大きさが、指紋の凹凸を反映して変化する。この電位低下ΔＶが、入力信号として出力回路８４０に供給されるので、出力回路８４０でΔＶが入力され、指紋の凹凸を反映した信号が出力される。こうした出力回路８４０の出力信号が処理装置２４により処理され、前述の指紋画像データとして生成される。

【００５０】

なお、実施の形態の１，２では、図４、図５を用いて動作例を説明してきたが、動作の順序を変更しても全体の動作に矛盾をきたさない場合は、動作の順序を変更してもよい。また、実施の形態の１，２では、携帯型端末装置１をネットワークとの通信手段を有するものとしているが、携帯可能なスタンドアロンのコンピュータとしてもよい。この場合にも、正規ユーザ以外の第三者による個人情報やサービス情報への不正アクセスを防止することができる。また、実施の形態の１，２では、携帯型端末装置１とネットワークとの間の通信を無線通信としているが、有線通信でもよい。また、携帯型端末装置１と生体認証装置２との間の通信を有線通信としているが、無線通信でもよい。

【００５１】

また、実施の形態の１～３では、生体情報として指紋を用いる場合を例に挙げて説明しているが、他の生体情報としては、例えばユーザの声紋、虹彩、筆跡、手形、指の長さ、人相などがある。生体情報としてユーザの手形又は指の長さを用いる場合、生体認証装置２のセンサ２２は、ユーザの掌又は指の画像を取り込み、処理装置２４は、取り込んだ画像データを記憶装置２３に予め登録された正規ユーザの掌又は指の画像データと照合する。

【００５２】

また、生体情報としてユーザの声紋、すなわちサウンドスペクトログラムを用いる場合、生体認証装置２のセンサ２２は、ユーザの音声を集音して声紋を抽出し、処理装置２４は、抽出した声紋のデータを記憶装置２３に予め登録された正規ユーザの声紋データと照合する。生体情報としてユーザの筆跡を用いる場合、生体認証装置２のセンサ２２は、ユーザのペン軌跡を取り込み、処理装置２４は、取り込んだ筆跡の画像データを記憶装置２３に予め登録された正規ユーザの筆跡データと照合する。

【００５３】

また、生体情報としてユーザの虹彩を用いる場合、生体認証装置２のセンサ２２は、ユーザの虹彩を撮影し、処理装置２４は、撮影した虹彩の画像データを記憶装置２３に予め登録された正規ユーザの虹彩の画像データと照合する。生体情報としてユーザの人相を用いる場合、生体認証装置２のセンサ２２は、ユーザの

顔を撮影して顔の特徴を抽出し、処理装置２４は、抽出した特徴データを記憶装置２３に予め登録された正規ユーザの特徴データと照合する。

【００５４】

【発明の効果】

本発明によれば、個人情報が生体認証装置に格納され、生体情報による本人認証の結果がＯＫの場合のみ、携帯型端末装置に個人情報が送出される。このため、正規ユーザ以外の第三者がパスワードを不正に取得したとしても、生体情報による本人認証の段階で携帯型端末装置への個人情報送出が拒否されるので、第三者は、携帯型端末装置から個人情報を不正に取得することはできない。したがって、パスワードの不正取得による個人情報への不正アクセスを防止することができ、セキュリティを向上させることができる。また、１つの生体認証装置を複数の携帯型端末装置に使うことができるので、ユーザは、個人情報の管理・編集を生体認証装置に対してのみ行えばよく、ユーザにとっての利便性とセキュリティとを向上させることができる。

【００５５】

また、サービス情報が生体認証装置に格納され、生体情報による本人認証の結果がＯＫの場合のみ、携帯型端末装置にサービス情報が送出される。このため、正規ユーザ以外の第三者がパスワードを不正に取得したとしても、生体情報による本人認証の段階で携帯型端末装置へのサービス情報送出が拒否されるので、第三者は、携帯型端末装置からサービス情報を不正に取得することはできない。したがって、パスワードの不正取得によるサービス情報への不正アクセスを防止することができ、セキュリティを向上させることができる。また、１つの生体認証装置を複数の携帯型端末装置に使うことができるので、ユーザは、サービス情報の管理・編集を生体認証装置に対してのみ行えばよく、ユーザにとっての利便性とセキュリティとを向上させることができる。また、第三者は、正規ユーザになりすましてサービス提供を受けることができなくなるので、セキュリティを向上させることができる。

【００５６】

また、本実施の形態では、個人識別番号が生体認証装置に格納されており、生

体情報による本人認証の結果がＯＫの場合のみ、携帯型端末装置に個人識別番号が送出されて付与される。このため、ユーザは、複数の携帯型端末装置を１つの個人識別番号で使用することができ、ユーザにとっての利便性を向上させることができる。また、正規ユーザ以外の第三者が正規ユーザの携帯型端末装置と生体認証装置とを不正に取得したとしても、生体情報による本人認証の段階で携帯型端末装置への個人識別番号送出が拒否されるので、第三者は、携帯型端末装置を使用することができない。したがって、セキュリティを向上させることができ、携帯型端末装置が不正に使用されて正規ユーザに課金がなされるといった問題を防ぐことができる。

【００５７】

また、ウエブサイトにログインする際に使用されるパスワードが生体認証装置に格納されており、生体情報による本人認証の結果がＯＫの場合のみ、携帯型端末装置にパスワードが送出されて、携帯型端末装置からウエブサイトにパスワードが送出される。正規ユーザ以外の第三者が携帯型端末装置を操作したとしても、生体情報による本人認証の段階で携帯型端末装置へのパスワード送出が拒否されるので、第三者は、正規ユーザになりすまして電子商取引を行うことはできない。したがって、セキュリティを向上させることができる。

【図面の簡単な説明】

【図１】　本発明の第１の実施の形態となる携帯型端末システムの外観図である。

【図２】　本発明の第１の実施の形態における携帯型端末装置の構成を示すブロック図である。

【図３】　本発明の第１の実施の形態における生体認証装置の斜視図及びブロック図である。

【図４】　本発明の第１の実施の形態となる携帯型端末システムの動作を示すフローチャート図である。

【図５】　本発明の第２の実施の形態となる携帯型端末システムの動作を示すフローチャート図である。

【図６】　生体認証装置内のセンサの検出素子の概略的な断面を示す図であ

る。

【図７】　図６のセンサの回路図である。

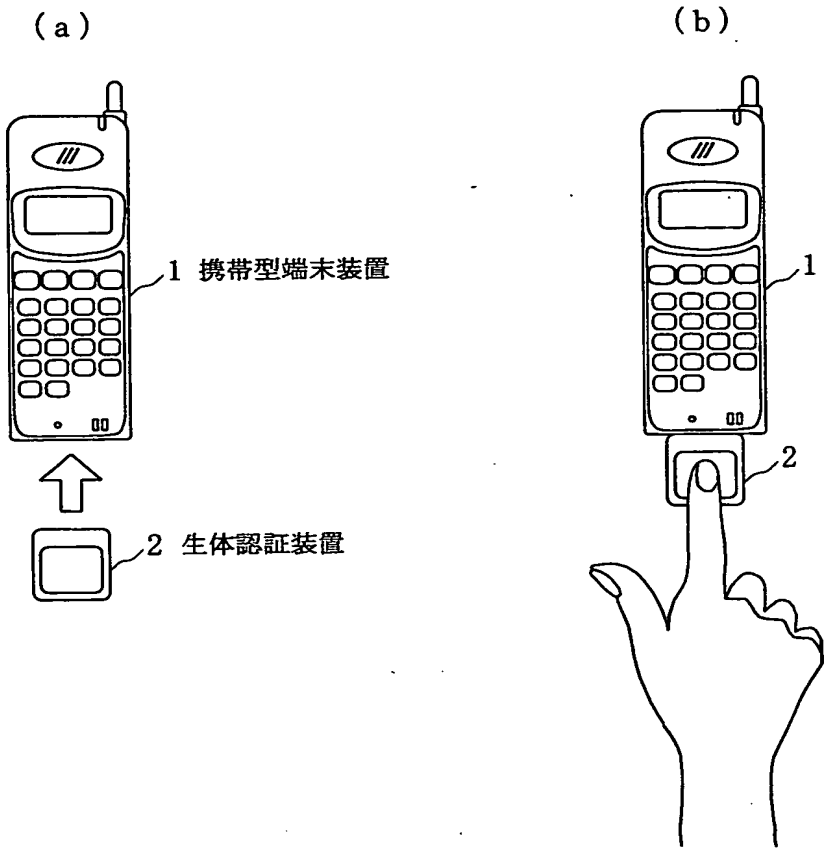
【図８】　図７に示したセンサの動作を説明するためのタイミングチャートである。

【符号の説明】

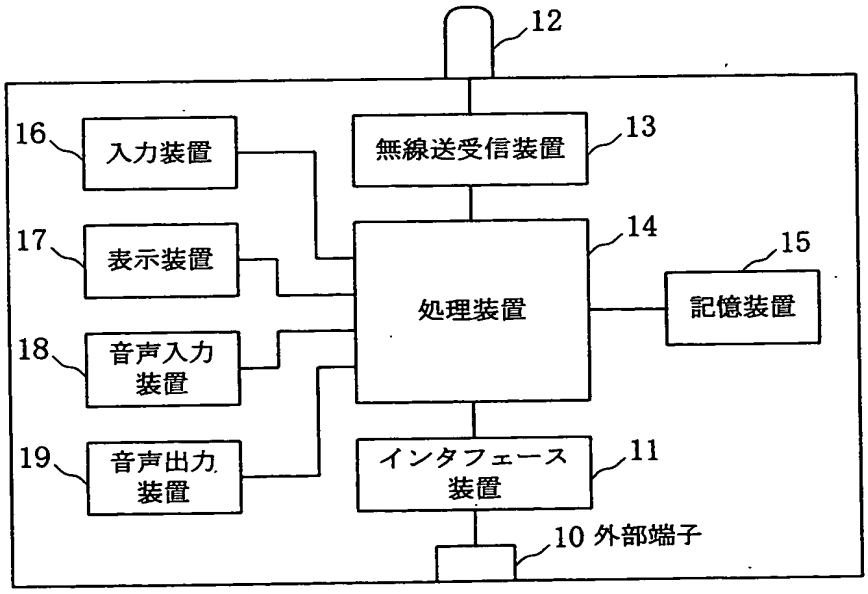
１…携帯型端末装置、２…生体認証装置、１０、２０…外部端子、１１、２１…インタフェース装置、１２…アンテナ、１３…無線送受信装置、１４、２４…処理装置、１５、２３…記憶装置、１６…入力装置、１７…表示装置、１８…音声入力装置、１９…音声出力装置、２２…センサ。

【書類名】　　図面

【図１】

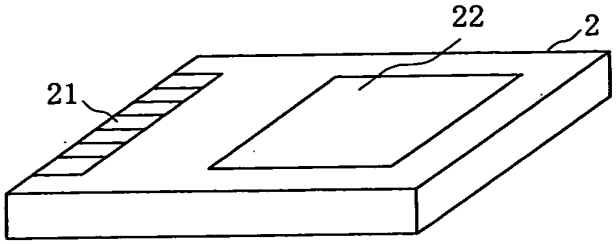

（ａ）
（ｂ）
1 携帯型端末装置
2 生体認証装置
1
2

【図２】

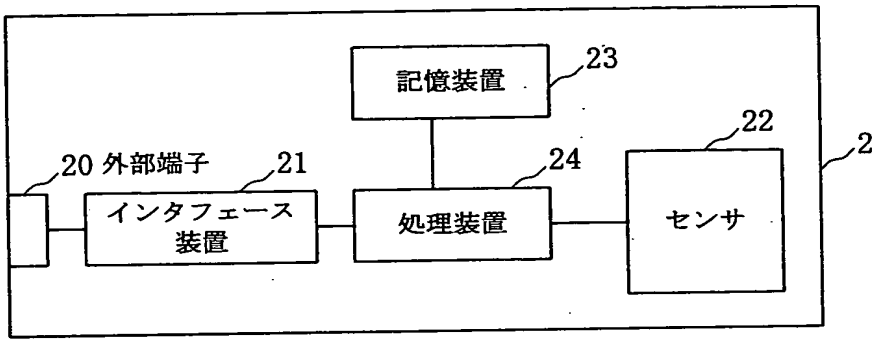

12
16
入力装置
無線送受信装置
13
17
表示装置
14
15
処理装置
記憶装置
18
音声入力
装置
19
音声出力
装置
インタフェース
装置
11
10 外部端子

【図３】

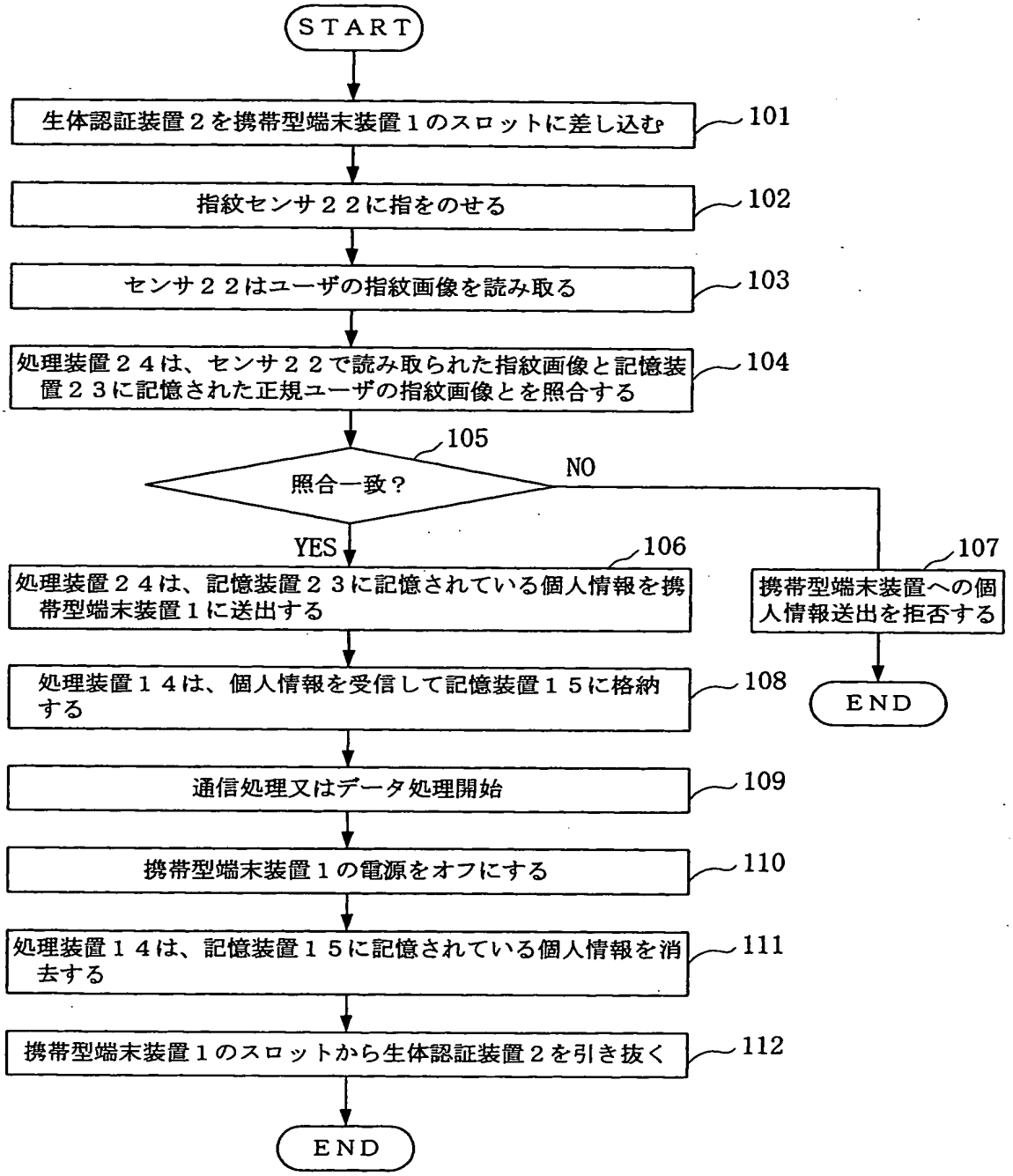
（ａ）



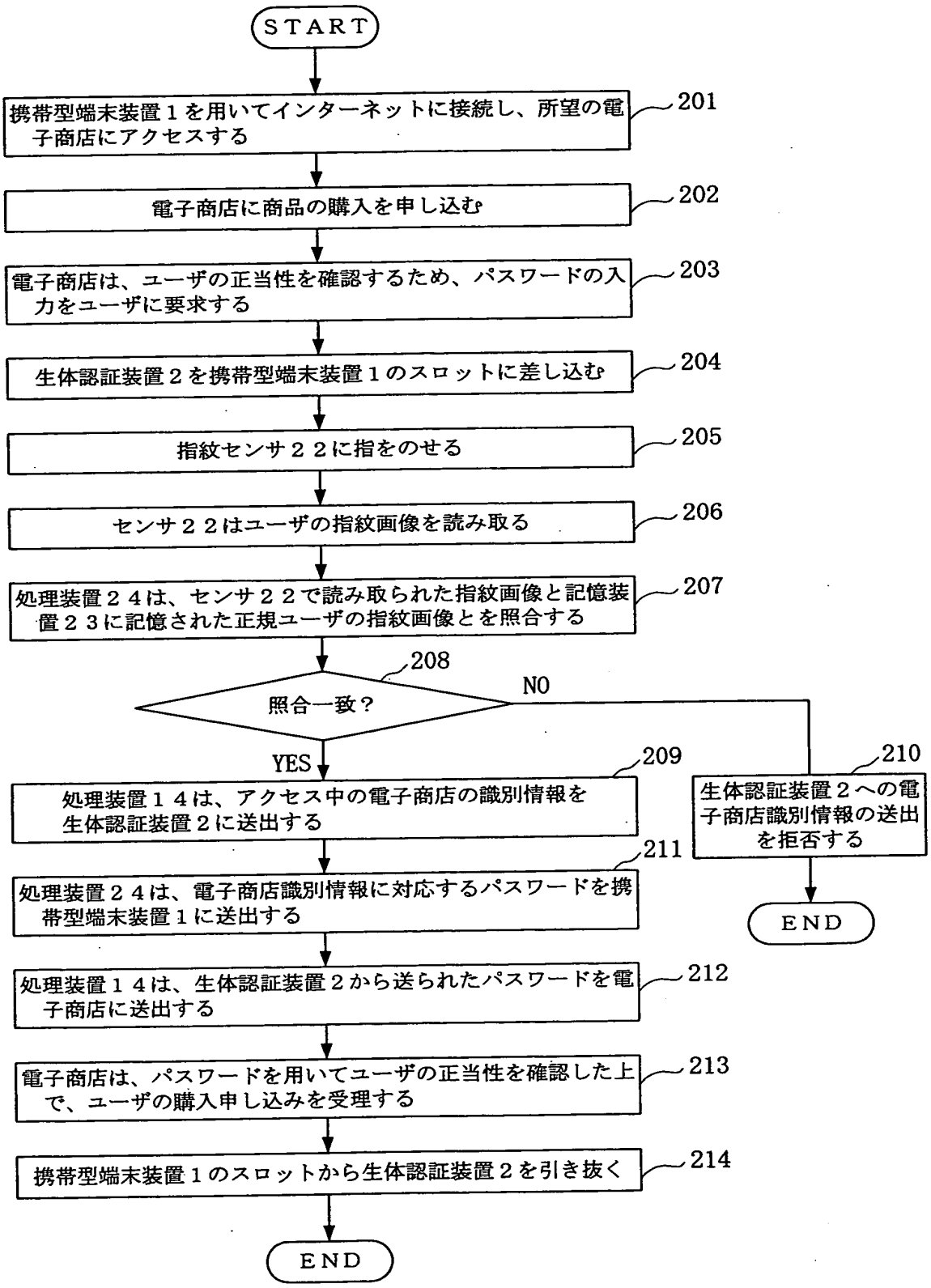
（ｂ）



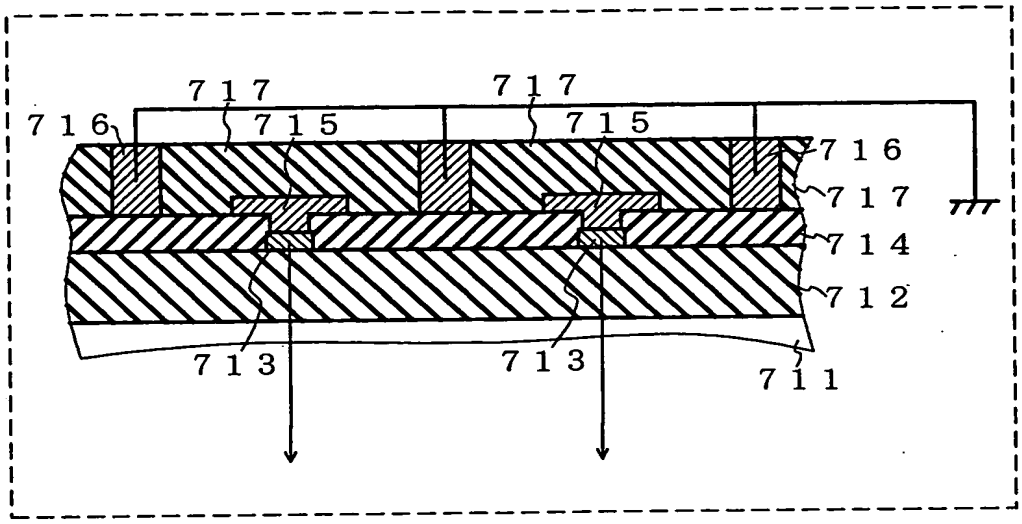
【図４】


START
生体認証装置２を携帯型端末装置１のスロットに差し込む
101
指紋センサ２２に指をのせる
102
センサ２２はユーザの指紋画像を読み取る
103
処理装置２４は、センサ２２で読み取られた指紋画像と記憶装置２３に記憶された正規ユーザの指紋画像とを照合する
104
105
照合一致？
NO
YES
106
処理装置２４は、記憶装置２３に記憶されている個人情報を携帯型端末装置１に送出する
107
携帯型端末装置への個人情報送出を拒否する
END
処理装置１４は、個人情報を受信して記憶装置１５に格納する
108
通信処理又はデータ処理開始
109
携帯型端末装置１の電源をオフにする
110
処理装置１４は、記憶装置１５に記憶されている個人情報を消去する
111
携帯型端末装置１のスロットから生体認証装置２を引き抜く
112
END

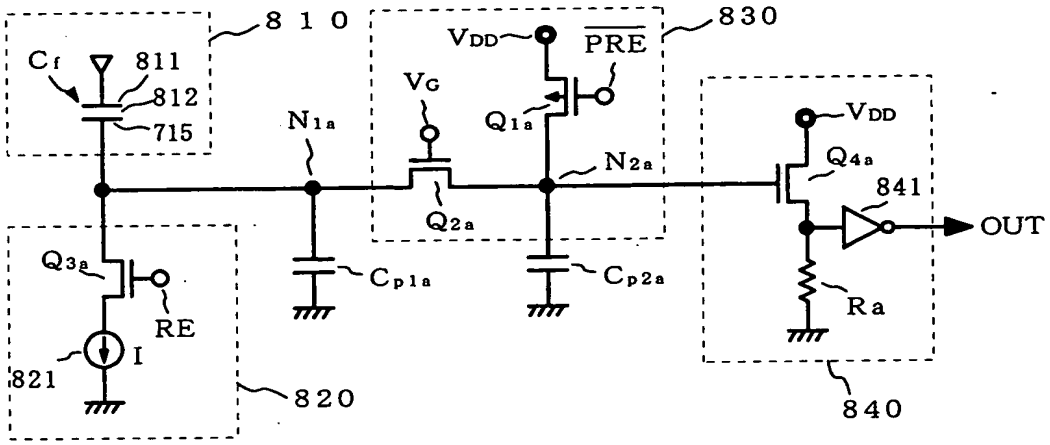
【図５】


START
携帯型端末装置１を用いてインターネットに接続し、所望の電子商店にアクセスする
201
電子商店に商品の購入を申し込む
202
電子商店は、ユーザの正当性を確認するため、パスワードの入力をユーザに要求する
203
生体認証装置２を携帯型端末装置１のスロットに差し込む
204
指紋センサ２２に指をのせる
205
センサ２２はユーザの指紋画像を読み取る
206
処理装置２４は、センサ２２で読み取られた指紋画像と記憶装置２３に記憶された正規ユーザの指紋画像とを照合する
207
208
照合一致？
NO
YES
209
処理装置１４は、アクセス中の電子商店の識別情報を生体認証装置２に送出する
210
生体認証装置２への電子商店識別情報の送出を拒否する
END
211
処理装置２４は、電子商店識別情報に対応するパスワードを携帯型端末装置１に送出する
212
処理装置１４は、生体認証装置２から送られたパスワードを電子商店に送出する
213
電子商店は、パスワードを用いてユーザの正当性を確認した上で、ユーザの購入申し込みを受理する
214
携帯型端末装置１のスロットから生体認証装置２を引き抜く
END

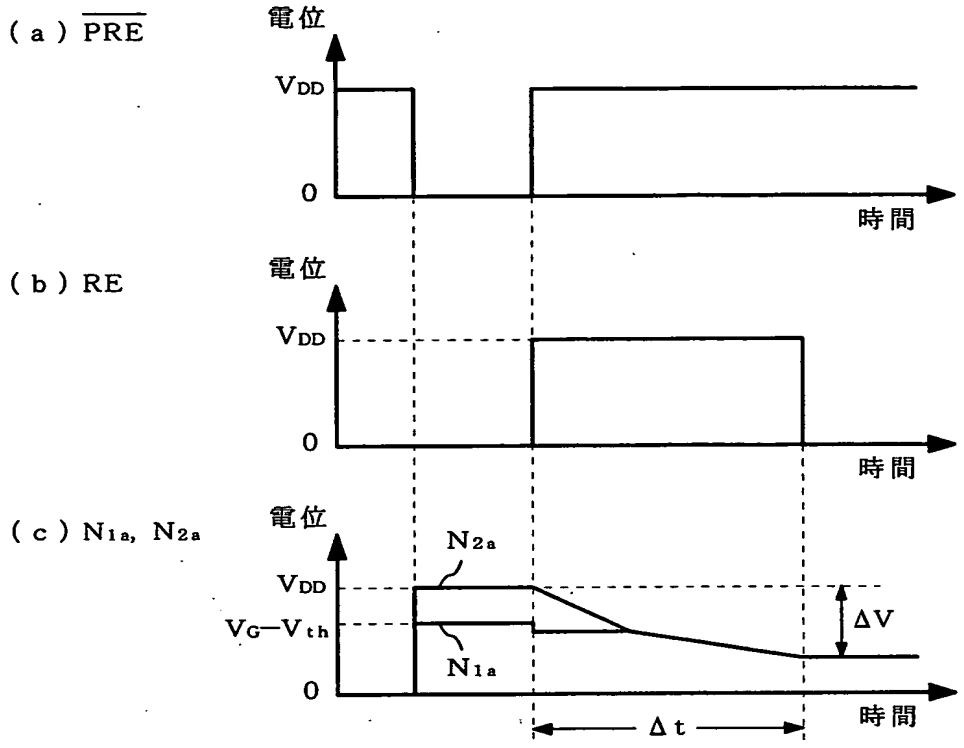
【図６】


７１７
７１５
７１６
７１３
７１１
７１４
７１２

【図７】


８１０
Cf
811
812
715
N1a
VG
VDD
PRE
Q1a
830
N2a
Q2a
Cp1a
Cp2a
Q3a
RE
I
821
820
VDD
Q4a
841
OUT
Ra
840

【図８】


(a) $\overline{PRE}$
電位
V_{DD}
0
時間
(b) RE
電位
V_{DD}
0
時間
(c) N_{1a}, N_{2a}
電位
N_{2a}
V_{DD}
V_G-V_{th}
N_{1a}
0
ΔV
Δt
時間

【書類名】　　要約書

【要約】

【課題】　個人情報の漏洩と不正な電子商取引とを防止する。

【解決手段】　生体認証装置２は、ユーザの生体情報を読み取る生体情報読取手段と、予め登録された正規ユーザの生体情報とこの正規ユーザの個人情報とを記憶する第１の記憶手段と、生体情報読取手段で読み取られた生体情報と第１の記憶手段に記憶された正規ユーザの生体情報とを照合して本人認証を行い、認証結果が照合一致を示す場合のみ、第１の記憶手段に記憶された個人情報を携帯型端末装置に送信する第１の処理装置とを有する。携帯型端末装置１は、送信された個人情報を記憶する第２の記憶手段と、第２の記憶手段に記憶された個人情報を用いて通信処理又はデータ処理を行う第２の処理手段とを有する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４２２６〕

１．変更年月日　　１９９９年　７月１５日
〔変更理由〕　住所変更
住　所　東京都千代田区大手町二丁目３番１号
氏　名　日本電信電話株式会社